International Journal of Engineering Research
Volume No.4, Issue No.4, pp : 165-172
ISSN:2319-6890(online),2347-5013(print)
01 April 2015

Hiding of Speech based on Chaotic Steganography and Cryptography Techniques

Abbas Salman Hameed
Assistant Lecturer, Electronic Engineering Department, College of Engineering, Diyala University,Iraq
Email: abbasfuture@yahoo.com

Abstract: The technique of embedding secret information into cover media, like image, video, audio and text called Steganography, so that only the sender and the authorized recipient who have a key can detect the presence of secret information. In this paper Steganography and Cryptography techniques of speech present with Chaos. Fractional order Lorenz and Chua systems that provides an expanded in key space are used to encrypt speech message. The large key space addition to all properties of randomness and nonlinearity which are possessed these chaotic systems ensure a highly robustness and security for cryptography process. As well as Modified Android Cat Map (MACM) offers additional space and security for steganography process. The irregular outputs of the MACM are used in this paper to embed a secret message in a digital cover image. The results show a large key sensitivity to a small change in the secret key or parameters of MACM. Therefore, highly security hiding for speech will be guaranteed by using this system.

Key Words: Steganography, Cryptography, Fractional Order chaotic system, Modified Android Cat Map

1. Introduction:

In the digital world, data is the heart of computer communication and global economy. To ensure the security of the data, the concept of data hiding has attracted people to come up with creative solutions to protect data from falling into wrong hands [1].

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message. Steganography works by replacing bits of useless or unused data (embedded) in regular computer files (such as graphics, sound, text, or HTML) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images [2]. To add more security, the data to be hidden is encrypted with a key during the embedding process. To extract the hidden information, one should have the key.

Steganography and cryptography are the two different information hiding techniques which provide confidentiality and integrity of data. Steganography technique aims at transmitting a message on a channel. The goal of steganography is to hide messages inside other "harmless" digital media in a way that does not allow any person to even detect the presence of secret message. Cryptography hides the contents of a secret message from an unauthorized people but the content of the message is visible. In cryptography, the structure of a message is scrambled in such a way as to make it meaningless and unintelligible manner [1,3].

For Cryptography process, Chaos is a typical behavior of nonlinear dynamic systems. It is characterized by extremely sensitive to parameters and initial conditions, mathematically defined as randomness governed by simple deterministic rules [4]. A high dimensional chaotic system like Lorenz or Chua system will give a more complex structure, more system variables, and parameters. Then the cryptosystem's key space will be larger for integer orders, and the system variables time sequence will be more erratic and unpredictable than using the low dimension chaotic system [5].

This paper demonstrates Encryption of speech using fractional order chaotic systems (Non integer orders) to increase the security level of generated key then embedded the encrypted data in cover image after applied Modified Arnold Cat Map (MACM) to shuffle the image pixels before embedded process.

The paper is organized as follows; section 2 describes the Fraction Order Lorenz and Chua systems and the Chaotic Key Generation. Section 3 shows the embedded process using MACM. The system model of steganography and encrypted speech is presented in section 4. In section 5, the simulation results of hiding and encryption speech message using chaos are presented. Finally, conclusions are presented in section 6.

2. Chaotic Cryptography:

Chaos is one of the possible behaviors associated with evolution of a nonlinear physical system and occurs for specific values of system parameters.

Chaotic systems have many important properties, such as the sensitive dependence on initial conditions and system parameters, pseudorandom property, no periodicity and topological transitivity, etc. Most properties meet some requirements such as diffusion and mixing in the sense of cryptography. Therefore, chaotic cryptosystems have more useful and practical applications [6].

Chaotic systems can be divided into those described by differential equations, known as flows such as: Lorenz System [7], Rössler System [8], Chua system [9]. And those described by difference equations, known as maps such as: logistic map [8], Hénon map [10], Arnold Cat Map (ACM) [11], … etc.

2.1 Fraction Order Lorenz and Chua systems:

The mathematical description of the fractional-order Lorenz system is expressed as [5]:

$$\begin{cases} D^{\alpha 1}x = \sigma_L(y - x) \\ D^{\alpha 2}y = -xz + \rho_L x - y \\ D^{\alpha 3}z = xy - \beta_L z \end{cases} \quad (1)$$

where (σ_L, ρ_L, β_L) are system parameters ,($\alpha 1$, $\alpha 2$ and $\alpha 3$) determine the fractional orders of the equation and ($\alpha 1$, $\alpha 2$,

ISSN:2319-6890(online),2347-5013(print)
01 April 2015

$\alpha 3 > 0$) . When $\alpha 1 = \alpha 2 = \alpha 3 = 1$, Eq. 1 becomes the ordinary integer orders Lorenz system.

Whereas, the mathematical description for fractional-order Chua system [12], can be expressed as:

$$\begin{cases} D^{\gamma 1}x = \sigma_C(y - x) - \sigma_C F(x) \\ D^{\gamma 2}y = x - y + Z \\ D^{\gamma 3}z = -(\rho_C y + \beta_C Z) \\ F(x) = m_1 x + (m_0 - m_1) * (|x + 1| - |x - 1|) \end{cases} \quad (2)$$

where (σ_C, ρ_C, β_C, m_0, m_1) are system parameters ,($\gamma 1$, $\gamma 2$ and γ 3) determine the fractional orders of the equation and ($\gamma 1$, $\gamma 2$, $\gamma 3 > 0$).

The solution of fractional-order Lorenz system using Fractional Backward Difference Methods [13] can be written as:

$$\begin{cases} x_m = h^{\alpha 1} * [\sigma_L * (y_{m-1} - x_{m-1})] - \sum_{k=1}^{m} w_k x(m - k_h) \\ y_m = h^{\alpha 2} * [-z_{m-1} * x_{m-1} + \rho_L * x_{m-1} - y_{m-1}] \ \ldots \\ \qquad \ldots \ - \sum_{k=1}^{m} w_k y(m - k_h) \\ z_m = h^{\alpha 3} * [x_{m-1} * y_{m-1} - \beta_L * z_{m-1}] - \sum_{k=1}^{m} w_k z(m - k_h) \end{cases} \quad (3)$$

And for Chua system can be written as:

$$\begin{cases} x_m = h^{\gamma 1} * [\sigma_C * (y_{m-1} - x_{m-1}) - \sigma_C * F(x)] \ \ldots \\ \qquad \ldots \ - \sum_{k=1}^{m} w_k x(m - k_h) \\ y_m = h^{\gamma 2} * [x_{m-1} - y_{m-1} + z_{m-1}] \ \ldots \\ \qquad \ldots \ - \sum_{k=1}^{m} w_k y(m - k_h) \\ z_m = h^{\gamma 3} * [-\rho_C * y_{m-1} - \beta * z_{m-1}] - \sum_{k=1}^{m} w_k z(m - k_h) \end{cases} \quad (4)$$

where h, is step size parameter and m = 0,1,2,..,N. The coefficients w_k can be computed in a recursive scheme (with w_0 = 1) by

$$w_k = \left(1 - \frac{\varphi + 1}{k}\right) w_{k-1} \quad (5)$$

where φ, is α or γ order corresponding to chaotic sequence type.

2.2 Chaotic Key Generation:

To generate chaotic key used to encrypt the speech message, the sequences generated from fraction-order Lorenz system and fraction-order Chua system are pre-processing by magnification and modulo transformation to the two chaos types sequences as:

$$\begin{cases} M_L(n) = mod(floor(M_L(n) \times 10^{15}), 2^N) \ \ for\ Lorenz \\ M_C(n) = mod(floor(M_C(n) \times 10^{16}), 2^N) \ \ for\ Chua \end{cases} \quad (6)$$

where M_L and M_C, are (x, y, z) sequences for Lorenz and Chua respectively. N is maximum number of bits required to quantize M into an integer sequence.

Then, to make proposed system more secure, the fractional-order of Lorenz and Chua sequences are combined together by using XOR to get new chaotic sequences as in Eq. 7.

$$\begin{cases} K_1(n) = BITXOR(x_L(n), y_C(n), z_L(n)) \\ K_2(n) = BITXOR(x_C(n), y_L(n), z_C(n)) \\ K_3(n) = BITXOR(x_L(n), x_C(n)) \end{cases} \quad (7)$$

The combined of these sequences are improved the security level of the system by enhancing the encryption process complexity, the key space and the robustness of the cryptosystem.

To get highly random and uncorrelated key, K_1(n) and K_2(n) are fed to a 2×1 multiplexer which dynamically selects one of randomly key dependent on random value of K_3(n) to produce the next member of output keystream as shown in Fig. 1.

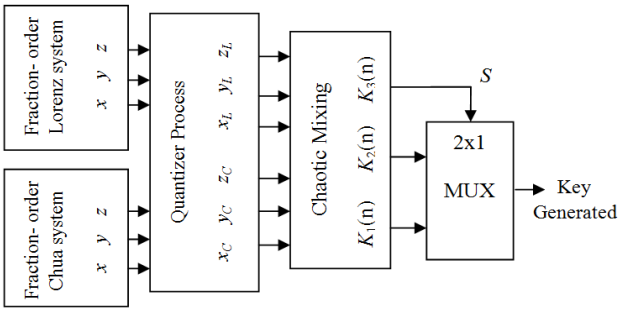


Fig. 1 Block diagram of Chaotic Key Generation.

3. Embedded Data using ACM:

Digital covers have a large number of redundant bits such least significant bits (LSB). In the substitution technique of steganography, the bits of the secret message substitute the LSB of the bytes of the cover file without causing a drastic change to this cover file [14]. To increase the security of embedded process, a secret message is embedded in the irregular output pixels of the Arnold Cat Map (ACM) that is applied on a digital cover image.

ACM is used in the embedding process in order to improve the image hiding safety and visual quality of the extracted message. Which when applied to a digital image randomizes the original organization of its pixels and the image becomes imperceptible or noisy. So, the secret message will become chaotic on the embedding process and if the receiver side wants to extract the secret message it should know the exact location which was used for embedding. In this way, it is becoming exponentially hard to recover the initial message without knowing the original transformation or the secret key. However, ACM has a period p to shuffle image pixels and if iterated p number of times, the original image reappears [15].

The generalized form of ACM can be given by the transformation [15].

$\Gamma : T^2 \rightarrow T^2$ such that:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \text{ (mod N)} \quad (8)$$

where, x, y $\{0, 1, 2 \ldots N-1\}$ and N is the size of a digital image.

It can easily be seen that the original Arnold transformations given by Eq. 8 can be modified to produce a sequence of Modified Arnold Cat Map (MACM) [15] by introducing new three parameters (a,b,c) to increase and ensure high security implementation as:

ISSN:2319-6890(online),2347-5013(print)
01 April 2015

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{bmatrix} 1 & b+c^2 \\ a & 1+a\,b+a\,c^2 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod N \qquad (9)$$

where a,b and c are positive integer values considered as a control parameters and (a, b, c)$\in \mathbb{R}$, x' and y' are the coordinate values of the shuffled pixel.

4. SYSTEM MODEL:

The proposed system is shown in Fig.2. First, the speech signal is preprocessed and quantized to get the corresponding speech bitstream. The speech bitstream is then XORed with the chaotic Key generation as in section 2.2 to generate encrypted data.

Before embedded the encrypted speech message in image pixel, the cover image is permutated using MACM with *p* iteration and (a, b, c*)* parameters to increase and ensure high security implementation. After that, inverse process of Modified Arnold Cat mapping (IMACM) is done on the image to rearrangement the image coordinate values of the shuffled pixel, and then the result stego image is transmitted.

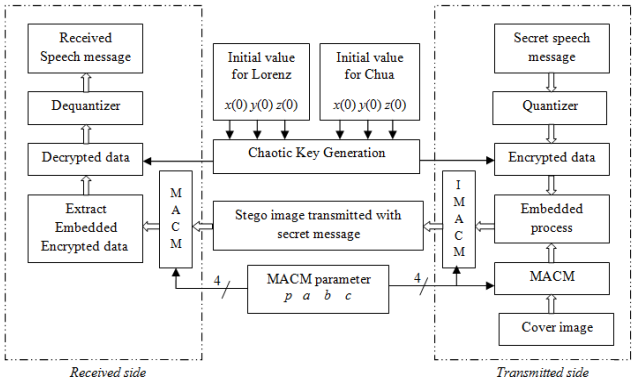


Fig. 2 Block Diagram of Proposed Hiding and Encryption Speech at Transmitted Side, Decryption and Extraction at Receiver Side**.**

At the receiver side, MACM must be performed on the received stego image to extracted encrypted data. Then the decrypted process is executed by the same chaotic key used in transmitted side.

5. Simulation Results:

The simulation uses the following referencing speech file: "*Army moves toward the enemy and should be fighting at zero moment*". The speech signal is sampled at 8 kHz and is quantized with 10 bits / sample, 58.6 k byte with respect to 60 *msec*., as shown in Fig. 3.

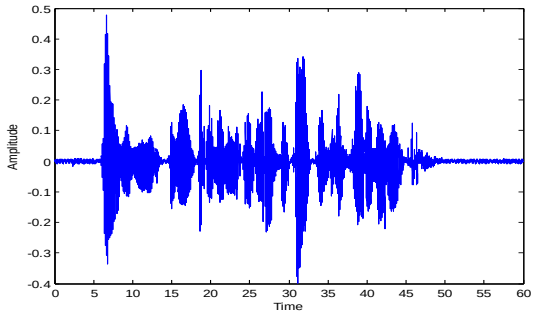


Fig. 3 Original Speech Signal.

In this simulation, Grayscale image of size 800x800 pixels is used as a cover image to test the proposed algorithm. The images used are shown in Fig.4.

Fig. 4 Grayscale Parrot Cover Image.

5.1 Test of Chaotic Cryptography:

The fraction-order Lorenz system used to generate secure chaotic key has these qualifications:- Fraction order: $\alpha 1=0.96$, $\alpha 2=0.98$, $\alpha 3=1.1$. The control parameters: $\sigma_L=10$, $\rho_L=28$, $\beta_L=8/3$. The initial conditions: $x(0)=0.1, y(0)=-0.1$, z $(0)=20$. Integer step-size: h=0.01.

And fraction-order Chua system is based on these qualifications:- Fraction order: $\gamma 1=0.97$, $\gamma 2=1$, $\gamma 3=1.01$. The control parameters: $\sigma_C=10$, $\rho_C=14.78$, $\beta_C=0.0385$, $m_0=-1.27$, $m_1=-0.68$. The initial conditions: $x(0)=0.2$, $y(0)=0.1$, $z(0)=0.1$. Integer step-size: h=0. 01. The encrypted and decrypted speech generated by using chaotic key has these parameters are shown in Fig. 5.

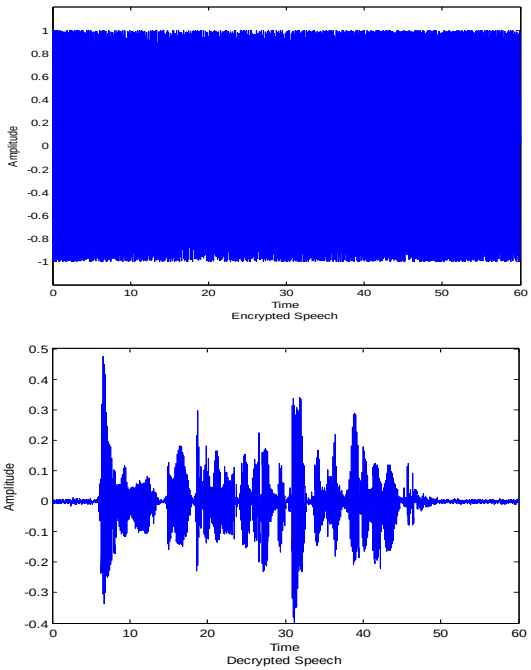


Fig. 5 Encrypted and Decrypted Speech using Chaotic Key.

5.1.1 Sensitivity to Fractional Orders:

The sequences response of Chaos is very sensitive to any small change in fraction-order values. To show that, for the Lorenz, *x* time response for two identical systems with the

ISSN:2319-6890(online),2347-5013(print)
01 April 2015

same parameters but starting from different fractional orders, 10^{-6} to be difference, is shown in Fig. 6.

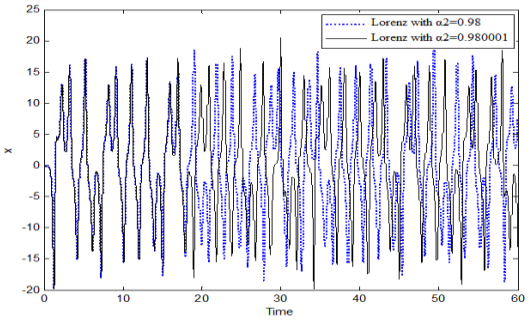


Fig. 6 Time series of variables *x* for Lorenz system**.**

As well, Fig. 7 shows *x* time response for two Chua system with the same parameters but starting from different fractional orders, 10^{-6} to be difference.

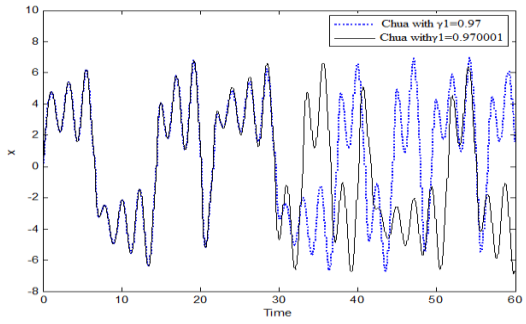
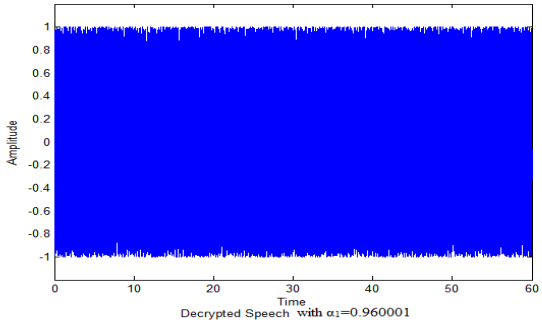
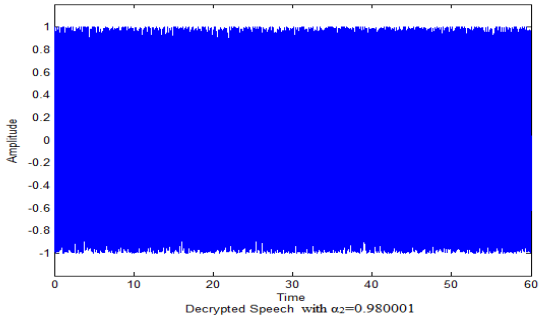


Fig. 7 Time series of variables *x* for Chua system**.**

Also, test effect of all fraction-order of Lorenz system on the decrypted speech signal is done. Fig. 8 shows the decrypted process of the signal that is generation with chaotic key has default parameters, with three chaotic keys have same parameters except only one parameter of key is changed at a time by 10^{-6} as α_1=0.960001, α_2=0.980001, and α_3=1.100001 respectively.





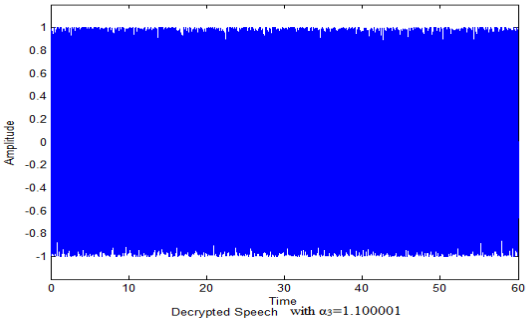
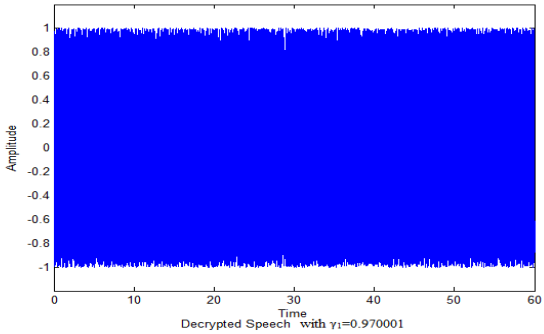
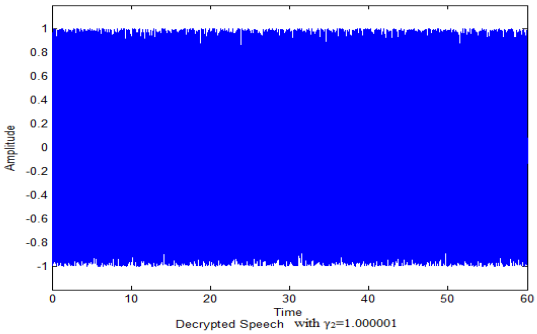


Fig. 8 Decrypted Process with Deference in Fraction-order of Lorenz α $+10^{-6}$**.**

To test the effect of all fraction-order of Chua system on the decrypted speech signal, three chaotic keys have same default parameters except only one parameter of key is changed at a time by $+10^{-6}$ as γ1=0.970001, γ2=1.000001, and γ3=1.010001 respectively as shown in Fig. 9.





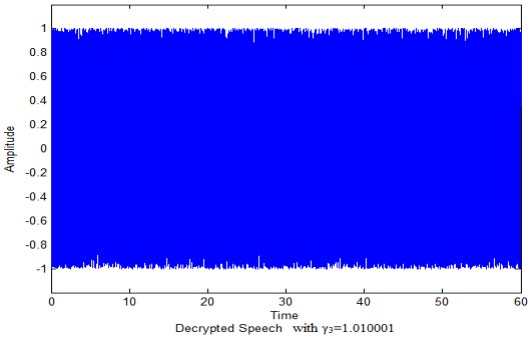


Fig. 9 Decrypted Process with Deference in Fraction-order of Chua γ $+10^{-6}$**.**

ISSN:2319-6890(online),2347-5013(print)
01 April 2015

5.1.2 Sensitivity to Initial Value:

To demonstrate the key sensitivity for initial values, first, Lorenz system is tested by changed one parameter only of Lorenz initial values at a time with a tiny amount of 10^{-6}, keeping all other parameters of chaotic key unchanged and the scheme is applied to recover the speech signal. And so, three chaotic keys will be tested in decrypted process, each of them only changes the one of initial vales as $x(0)$=0.100001, $y(0)$= -0.100001, and $z(0)$=20.000001 respectively. The results of demonstration are shown in Fig. 10.

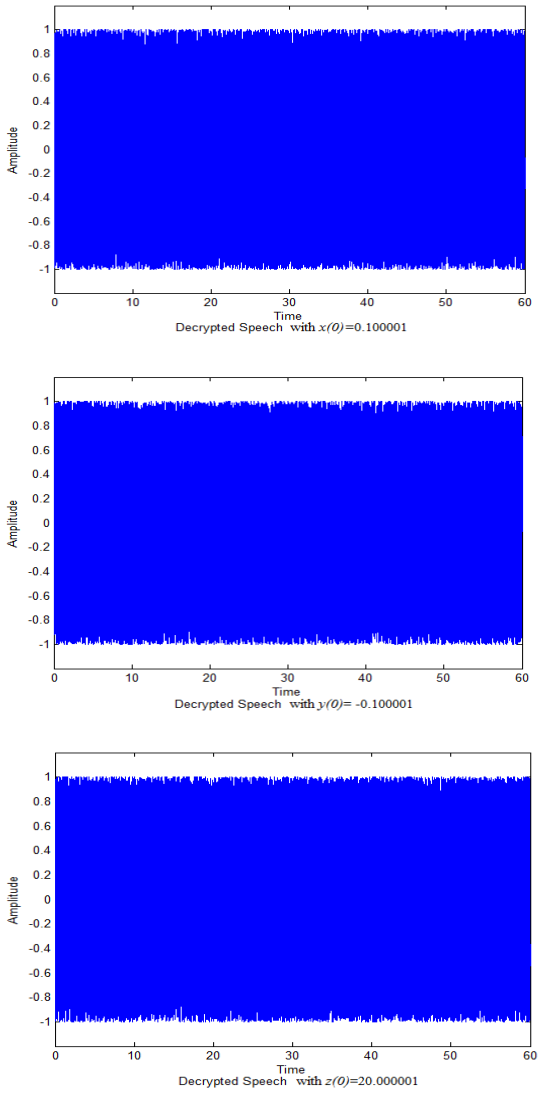


Fig. 10 Decrypted Process with Deference in Initial Values of Lorenz System**.**

As well, to show the key sensitivity for initial values of Chua system, three chaotic keys will be tested in decrypted process. Each of them only changes the one of initial vales at a time and keeping all other parameters of chaotic key unchanged as $x(0)$=0.200001, $y(0)$= 0.100001, and $z(0)$=0.100001 respectively. The results are shown in Fig. 11.

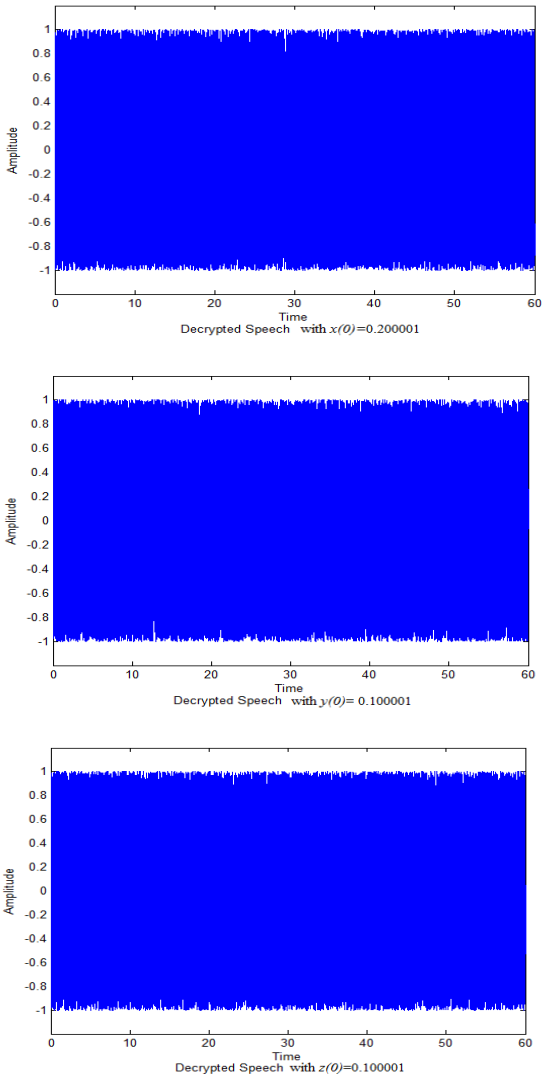
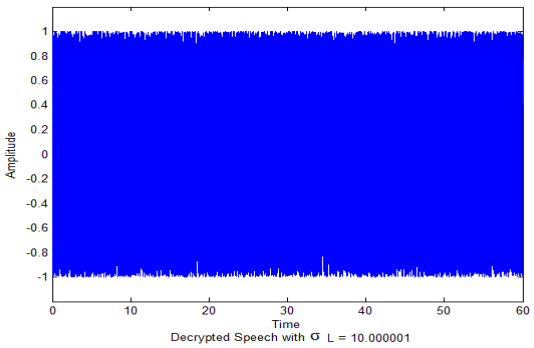


Fig. 11 Decrypted Process with Deference in Initial Values of Chua System**.**

5.1.3 Sensitivity to control parameters:

To test the effect of small change in control parameters for Lorenz or Chua system, Fig. 12 shows decrypted speech by the two chaotic key generated with small change in one control parameter at atime compared with defualt parameter used to generate chaotic key at transmitted side as σ_L=10.000001**,** ρ_C=14.780001 respectively, as example, at the received side.



ISSN:2319-6890(online),2347-5013(print)
01 April 2015

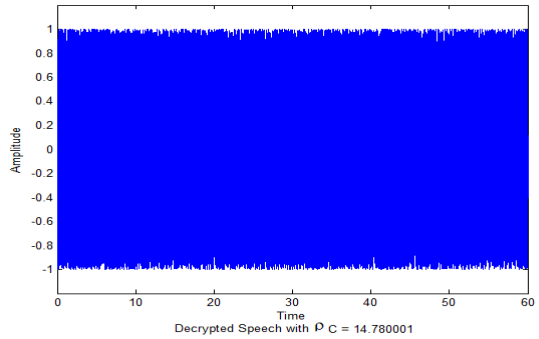


Fig. 12 Decrypted Process with Deference in σ_L, ρ_C of Lorenz and Chua System

Table 1, summarized the similarity between extracted secret speech message and original secret speech corresponding to a tiny amount of 10^{-6} change in one parameters only at a time for received chaotic key. The similarity is computed using normalized correlation *NC* between them according to Eq. 10.

$$NC = \frac{\sum_{k=1}^{QN} M(K)M'(K)}{\sqrt{\sum_{k=1}^{QN} M(K)^2}\sqrt{\sum_{k=1}^{QN} M'(K)^2}} \quad \textbf{(10)}$$

where M and M´ are original and extracted secret speech messages respectively, QN represents number of samples in each one of them [16]

Table 1, summarized the similarity between original and recovered speech.

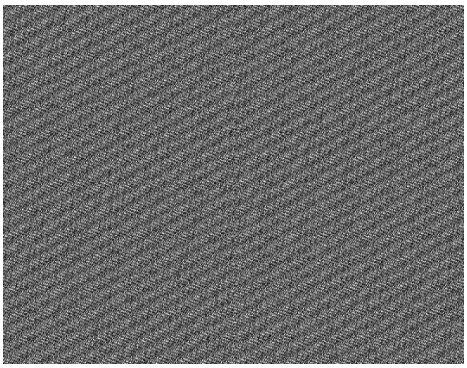
Parameter changed by 10^{-6}	*NC*	Parameter changed by 10^{-6}	*NC*
$\alpha 1$	-0.041	$\gamma 1$	-0.0022
$\alpha 2$	-0.0313	$\gamma 2$	-0.0056
$\alpha 3$	0.0034	$\gamma 3$	-0.015
$x(0)_{Lorenz}$	-0.0416	$x(0)_{Chua}$	-0.0022
$y(0)_{Lorenz}$	0.061	$y(0)_{Chua}$	-0.0123
$z(0)_{Lorenz}$	0.013	$z(0)_{Chua}$	0.0598
σ_L	0.0813	σ_C	0.081
ρ_L	0.0177	ρ_C	-0.003
β_L	0.005	β_C	-0.0029
No parameters changed *NC* = 1			

Table 1, shows highly sensitivity for a tiny change in any parameters of chaotic key system.

5.2 Test of Steganography Using MACM:

The Modified Arnold Cat Mapping (MACM) used to increase and ensure high security implementation for data hiding in images by introducing new parameters (a, b, c, and *p*) used to shuffle the coordinate values of cover image pixel to a new coordinates corresponding to these parameters and Eq. 9.

The values of MACM parameters will be used in this work are: a=2, b=3, c=5, and *p*=3 iteration. Fig. 13 shows the image generated by using MACM before embedded the encrypted speech message, the transmitted stego image with secret speech message, and decrypted speech extracted from received stego image after applied MACM on it.



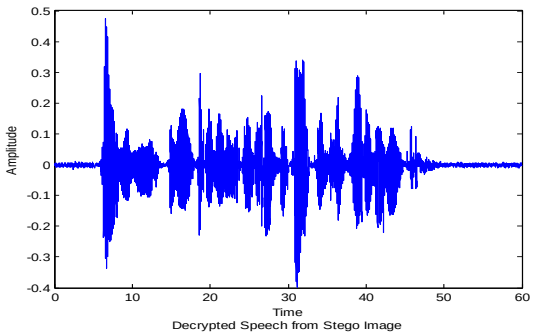


Fig. 13 MACM Image, Transmitted Stego Image, and received Speech**.**

From Fig.13, The received speech signal is similar to transmitted signal shown in Fig. 3 with *NC*=1 at used the same parameters of MACM and same chaotic key in the received side. Also, PSNR= 40.35 dB, calculated as in [15], for shown stego image.

To test the effect of incorrect control parameters of MACM, the image generated by using MACM at received side and decrypted speech extracted from it will be shown in Fig. 14 and Fig. 15. In each figure the stego image is processed with the same chaotic key and same parameters of MACM except only one parameter is changed at a time as a=3 and c=4, as example, respectively.

ISSN:2319-6890(online),2347-5013(print)
01 April 2015

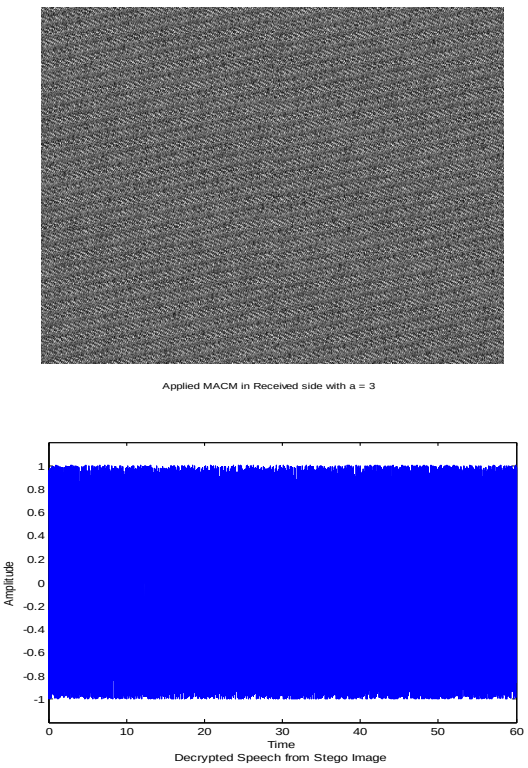


Fig. 14 MACM Image with a=3, and received Speech from it.

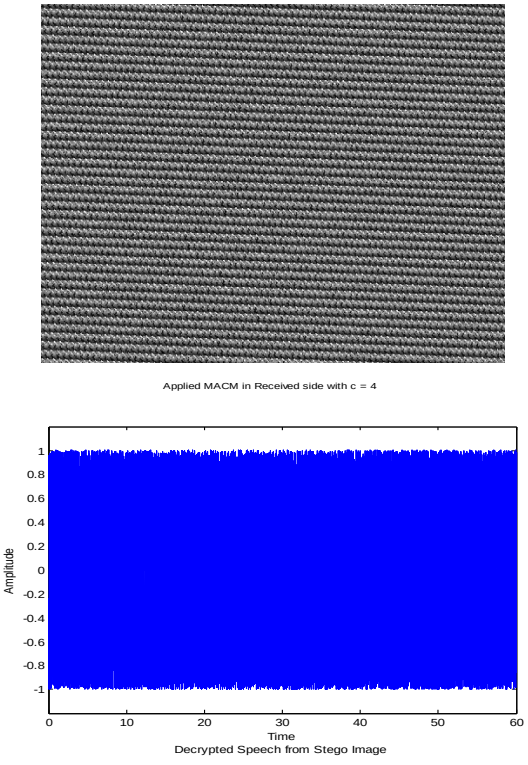


Fig. 15 MACM Image with c=4, and received Speech from it.

From these figures, extracted correct data from stego image in received side will be highly difficult process without used same MCAM parameters that is used in transmitted side.

5.3 Key Space and System Security:

Key space size is the total number of different keys that are used in the encryption. The chaotic key used in this work is highly sensitive to fraction- order for Lorenz ($\alpha1$, $\alpha2$, $\alpha3$) and Chua ($\gamma1$, $\gamma2$, $\gamma3$) systems, Lorenz parameters (σ_L, ρ_L, β_L), Chua parameters (σ_C, ρ_C, β_C, m_0, m_1), and also to initial values of the system. All parameters and initial conditions constitute the secret key of encryption system. Also, the (a, b, c) parameters and *p* iteration used in MACM to hiding the encrypted speech are provide addition system security space. Hence, the space of the key and system, in general, will be a very high dimensional space. Large secret key parameters space is very important to resist the exhaustive attack.

6. Conclusions:

In this paper, fractional derivative order of Lorenz and Chua are employed as a high dimensional chaotic system to generate more complex and unpredictable six chaotic sequences. These sequences used to produce highly complicated security chaotic key can be used in the secure cryptography and steganography of speech message. This system has a large key sensitivity because a small change in the secret key causes a large change in the decrypted signal as shown by low normalized correlation value when compared the similarity between extracted secret speech message using incorrect key with original secret speech. Also, additional security is guaranteed by using Modified Arnold Cat Map to hiding the speech message in image. With the use of fractional derivative order as the keys, and Modified Arnold Cat Map parameters makes the key space expanded and warranty to high security

References:

i. S. A. Laskar, and K. Hemachandran," Secure Data Transmission Using Steganography And Encryption Technique", International Journal on Cryptography and Information Security (IJCIS), vol.2, No.3, pp. 161-172, September 2012.

ii. B. Nagaria, A. Parikh, S. Mandliya, and N. shrivastav, " Steganographic Approach for Data Hiding using LSB Techniques", International Journal of Advanced Computer Research, vol. 2, No. 4, pp. 441-445, December 2012.

iii. R. Nivedhitha, T. Meyyappan, and M. Phil, " Image Security Using Steganography And Cryptographic Techniques", International Journal of Engineering Trends and Technology, vol. 3, pp. 366 – 371, 2012.

iv. S. H. Strogatz, "Nonlinear dynamics and chaos", PreseusBooks Publishing, LLC, 1994.

v. R. Nicholas, "Introduction to Lorenz's System of Equations", Math 6100, December 2003.

vi. K. Sakthidasan, and B. V. Santhosh," A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images," International Journal of Information and Education Technology, vol. 1, No. 2, pp. 137-141, June 2011.

vii. Edward N. Lorenz," Deterministic Nonperiodic flow",Massachusetts Institute of Technology ,Journal Of The Atmospheric Science ,Vol.20,1963.

viii. K. K. Kabi, C. Pradhan, B.J. Saha, and A. Kumar Bisoi, " Comparative study of image encryption using 2D chaotic map", Proceedings of IEEE, International Conference of Information Systems and Computer Networks, pp. 105 - 108, March 2014.

ix. Leon O. Chua, Chai W. Wu& A. Huang, "A Universal Circuit for Studying and Generating Chaos—Part I: Routes to Chaos", Circuits and Systems Fundamental Theory and Applications, IEEE Transactions, vol.40, pp.732-744,1993.

ISSN:2319-6890(online),2347-5013(print)
01 April 2015

x. M. Henon "A Two-Dimensional Mapping With A Strange Attractor", Springer-Verlag Communications In Mathematical Physics, Vol.50,pp.69-77,1976.

xi. V. Arnold, "mathematical methods of classical mechanics", springer Graduate Texts in Mathematics, Vol. 60,1985.

xii. Leon O. Chua, "The Genesis of Chua's Circuit", CiteSeerX - Scientific documents, vol. 46, No. 4, pp. 250–257, 1992.

xiii. K. Sun, and X. Wang, "Bifurcations and Chaos in Fractional Order Simplified Lorenz System", International Journal of Bifurcation and chaos, vol. 20, No. 4, pp. 1209–1219, 2010.

xiv. M. U. Celik, G.Sharma, A.M. Tekalp, and E. Saber, " Lossless generalized -LSB data embedding", Image Processing, IEEE Transactions, vol. 14, pp. 253 - 266, 2005

xv. M. Mishra, A. R. Routray, and S. Kumar", High Security Image Steganography with Modified Arnold's Cat Map ", International Journal of Computer Applications, vol. 37, No.9, Jane 2012.

xvi. Sreejith.V, Srijith.K, Rajesh Cherian Roy, " Robust Blind Digital Watermarking in Contourlet Domain ", International Journal of Computer Applications, vol. 58, No.12, November 2012.